STATE OF ALABAMA

Information Technology Guideline

Guideline 660-02G1: Router Security

1. INTRODUCTION:

Routers provide services that are essential to the secure operation of the networks they serve. Compromise of a router can lead to various security problems on the network served by that router and on other networks with which that router communicates. Examples include:

- Compromise of a router's route tables can result in reduced performance, denial of network communication services, and exposure of sensitive data
- Compromise of a router's access control can result in exposure of network configuration details or denial of service, and can facilitate attacks against other network components
- Poor router filtering configuration can reduce the overall security of an entire enclave, expose internal network components to scans and attacks, and make it easier for attackers to avoid detection

2. OBJECTIVE:

Establish a baseline configuration for network routers to help protect sensitive data, ensure data integrity, and facilitate secure cooperation between independent enclaves.

3. SCOPE:

These guidelines apply to routers owned and/or operated by the State of Alabama, and to routers utilized on any State network domain. This guideline is expected to become a standard, and the recommendations will become requirements, after a (to-be-determined) period of voluntary implementation. Organizations are encouraged to implement these guidelines as soon as practical.

4. GUIDELINES:

The following guidelines were adapted from the Defense Information Systems Agency (DISA) Network Infrastructure Security Technical Implementation Guide (STIG). Consult this DISA source document for further information that is not provided in this guideline. The DISA requirement/recommendation reference numbers (NETxxxx) are included here for cross-reference with the source document.

Download the DISA Network Infrastructure STIG at http://iase.disa.mil/stigs/stig/index.html.

4.1 ROUTE TABLE INTEGRITY

NET0400: Ensure neighbor authentication with IPSec or MD5 Signatures are implemented for interior routing protocols with all peer routers within the same or between Autonomous Systems (AS).

NET0402: Ensure neighbor authentication with IPSec Authentication Header (AH) is implemented between OSPFv3 (Open Shortest Path First) peer routers within the same or between AS.

NET0408: Ensure neighbor authentication with IPSec AH or MD5 signatures are implemented for all Border Gateway Protocol (BGP) routing protocols with all peer routers within the same or between Autonomous Systems.

NET0410: Restrict BGP connections to known IP addresses of neighbor routers from trusted Autonomous Systems.

NET0412: If multiple eBGP peers are defined in the network, ensure all eBGP neighbor authentications are configured with unique passwords when TCP MD5 Signature option is implemented.

4.2 KEY MANAGEMENT

NET0420: Ensure key management procedures have been implemented to include key generation, distribution, storage, usage, lifetime duration, and destruction of all keys used for encryption.

NET0422: Ensure a rotating key does not have a duration exceeding 180 days.

NET0425: Ensure the lifetime of MD5 Key expiration is set to never expire. The lifetime of the MD5 key will be configured as infinite for route authentication, if supported by the current approved router software version.

4.3 SECURING ROUTER PLANES

4.3.1 Operating System

NET0700: Implement the latest stable operating system on each router.

4.3.2 Cisco Discovery Protocol

NET0710: Ensure Cisco Discovery Protocol (CDP) is disabled on all external interfaces on Cisco premise routers.

4.3.3 Trivial Services

NET0720: Ensure TCP & UDP small servers are disabled.

NET0722: Ensure Packet Assembler Disassembler (PAD) services are disabled.

NET0726: Ensure identification support is disabled.

NET0730: Ensure Finger is disabled.

4.3.4 Idle Timeout Connections

NET0724: Ensure TCP Keep-Alives for Telnet Session are enabled.

4.3.5 HTTP, DHCP and FTP Server

NET0728: Ensure DHCP Services are disabled on premise routers.

NET0740: Ensure HTTP servers are disabled.

NET0742: Ensure FTP server is disabled.

4.3.6 BSD Remote Services

NET0744: Ensure all Berkeley Software Distribution (BSD) r-command servers are disabled.

4.3.7 Bootp Server

NET0750: Ensure Bootp server is disabled.

NET0760: Ensure configuration auto-loading is disabled.

4.3.8 IP Source Routing

NET0770: Ensure IP source routing is disabled.

4.3.9 Proxy and Gratuitous Address Resolution Protocol (ARP)

NET0780: Ensure Proxy ARP is disabled.

NET0781: Ensure Gratuitous ARP is disabled.

4.3.10 Directed Broadcasts

NET0790: Ensure IP directed broadcast is disabled on all router interfaces.

4.3.11 Internet Control Message Protocol (ICMP) Exploits

NET0800: Ensure ICMP unreachable notifications, mask replies, and redirects are disabled on all external interfaces of the premise router.

4.3.12 Logging Integrity

NET0810: Ensure the enclave has two Network Time Protocol (NTP) servers defined to synchronize time.

NET0811: Ensure the premise router is acting as an NTP server for only internal clients.

NET0812: Ensure all internal routers are configured to use the premise router to synchronize time in an external trusted NTP implementation.

NET0813: When the NTP source originates from an internal clock, ensure all routers use MD5 to authenticate the time source.

4.3.13 Name Server

NET0820: Ensure the DNS servers are defined if the router is configured as a client resolver.

4.3.14 Simple Network Management Protocol (SNMP) Service

NET0890: Restrict SNMP access to the router from only authorized internal IP addresses.

NET0892: Ensure SNMP is blocked at all external interfaces.

NET0894: Ensure SNMP is only enabled in the read mode; Read/Write is not enabled unless approved and documented by the IAO/NSO.

4.3.15 Loopback Source Address

NET0897: Ensure the router's loopback address is used as the source address when originating TACACS+ or RADIUS traffic.

NET0898: Ensure the router's loopback address is used as the source address when originating syslog traffic.

NET0899: Ensure the router's loopback address is used as the source address when originating NTP traffic.

NET0900: Ensure the router's loopback address is used as the source address when originating SNMP traffic.

NET0901: Ensure the router's loopback address is used as the source address when originating NetFlow traffic.

NET0902: Ensure the router's loopback address is used as the source address when originating TFTP or FTP traffic.

NET0903: Ensure the router's loopback address is used as the source address for BGP peering sessions.

4.4 PORTS, PROTOCOLS, AND SERVICES (PPS)

NET0910: Utilize ingress and egress access control lists (ACLs) to restrict traffic for all ports and protocols required for operational commitments.

NOTE 1: If the router is in a Deny-by-Default posture (strongly recommended) and what is allowed through the router filtering is required by operational necessity, and if the permit rule is explicitly defined with explicit ports and protocols allowed, then all requirements related to PPS being blocked would be satisfied.

NOTE 2: When the site is in an allow-all posture, all filter statements need to be verified and all PPS that are mandated to be blocked will need to have a rule created to block these ports and protocols.

4.4.1 ICMPv4 Message Types

NET0911: The System Administrator (SA) can permit inbound ICMP messages Echo Reply (type 0), ICMP Destination Unreachable - fragmentation needed (type 3 - code 4), Source Quench (type 4), Time Exceeded (type 11), and Parameter Problem (type 12). All other inbound ICMP messages are prohibited. Exception: All ICMP messages must be denied from external approved gateway addresses.

NET0912: The System Administrator can permit outbound ICMP messages Source Quench (type 4), Echo Request (type 8), and Time Exceeded (type 11). All other outbound ICMP messages are prohibited. Exception: All ICMP messages must be denied to external approved gateway addresses.

4.4.2 Traceroute

NET0918: Block all inbound traceroutes to prevent network discovery by unauthorized users.

4.4.3 Distributed Denial of Service (DDoS) Attacks

See Note 1 in section 4.4.

Block known DDoS attack ports. The example below shows access list rules for blocking several popular DDoS attack tools.

```
! the TRINOO DDoS systems
access-list 170 deny tcp any any eq 27665 log
access-list 170 deny udp any any eq 31335 log
access-list 170 deny udp any any eq 27444 log
! the Back Orifice systemb
access-list 170 deny udp any any eq 31337 log
! the Stacheldraht DDoS system
access-list 170 deny tcp any any eq 16660 log
access-list 170 deny tcp any any eq 65000 log
! the TrinityV3 system
access-list 170 deny tcp any any eq 33270 log
access-list 170 deny tcp any any eq 39168 log
! the T0rn rootkit system
access-list 170 deny tcp any any eq 47017 log
! the Subseven DDoS system and some variants
access-list 170 deny tcp any any range 6711 6712 log
access-list 170 deny tcp any any eq 6776 log
access-list 170 deny tcp any any eq 6669 log
access-list 170 deny tcp any any eq 2222 log
access-list 170 deny tcp any any eq 7000 log
```

4.5 IPv4 ADDRESS FILTERING

NET0920: Bind the ingress ACL filtering packets entering the network to the external interface on an inbound direction.

NET0921: Bind the egress ACL filtering packets leaving the network to the internal interface on an inbound direction.

NET0940: Restrict the premise router from accepting any inbound IP packets with a source address that contain an IP address from the internal network.

NET0923: Restrict the premise router from accepting any inbound IP packets with a local host loop back address (127.0.0.0/8).

NET0924: Restrict the premise router from accepting any inbound IP packets with a link-local IP address range (169.254.0.0/16).

NET0926: Restrict the premise router from accepting any inbound IP packets having a source field from BOGON, Martian IP addresses.

NET0927: Restrict the premise router from accepting any inbound IP packets having a source field from RFC1918 IP addresses.

NET0928: Have a procedure in place to check for changes and modify the BOGON/Martian list on a monthly basis.

4.6 UNICAST REVERSE-PATH FORWARDING

NET0949: Enable Cisco Express Forwarding (CEF) to improve router stability during a SYN flood attack to the network.

NET0950: Restrict the router from accepting any outbound IP packet that contains an illegitimate address in the source address field via egress ACL or by enabling Unicast Strick mode.

4.7 SYN FLOOD ATTACK – PROTECTING SERVERS OR LANS

NET0960: Implement TCP intercept features provided by the router or implement a filter to rate limit TCP SYN to protect servers from any TCP SYN flood attacks from an outside network.

4.8 SYN FLOOD ATTACK –PROTECTING THE ROUTER

NET0965: Set the maximum wait interval for establishing a TCP connection request to the router to 10 seconds or less, or implement a feature to rate-limit TCP SYN traffic destined to the router.

4.9 DEVICE MANAGEMENT

4.9.1 Out-of-band (OOB) Management

NET1623: Ensure all OOB management connections to the device require passwords.

NET1624: Ensure the console port is configured to time out after 10 minutes or less of inactivity.

NET1628: Ensure modems are not connected to the console port.

NET1629: Ensure the device auxiliary port is disabled if a secured modem providing encryption and authentication is not connected.

4.9.2 In-Band Management

NET1635: Limit the use of in-band management to situations where the use of OOB management would hinder operational commitments or when emergency situations arise. Approve the use of in-band management on a case-by-case and documented basis.

NET1636: Ensure all in-band management connections to the device require passwords.

NET1637: Ensure the device only allows in-band management sessions from authorized IP addresses from the internal network.

NET1638: Ensure in-band management access to the device is secured using a State-approved encryption method (e.g., AES, 3DES, SSH, or SSL).

NET1639: Ensure the timeout for in-band management access is set for no longer than 10 minutes.

NET1640: Configure the ACL that is bound to the VTY (Virtual Teletype/Terminal) ports to log permitted and denied access attempts.

Secure Shell Implementation:

NET1645: Ensure SSH timeout value is set to 60 seconds or less, causing incomplete SSH connections to shut down after 60 seconds or less.

NET1646: Ensure the maximum number of unsuccessful SSH login attempts is set to three, locking access to the router.

NET1647: Ensure SSH version 2 is implemented.

4.9.3 Simple Network Management Protocol (SNMP)

NET1650: Ensure IPSec is used to secure traffic between the network management workstation on State-managed LANs and all monitored devices sent via the Internet or other external network.

NET1660: Ensure the SNMP Version 3 Security Model (both MD5 packet authentication and encryption of the protocol data unit) is used across the entire network infrastructure.

NET1665: Ensure all SNMP community strings are changed from the default values.

NET1666: Ensure all SNMP community strings and usernames are protected via technology that secures using a State-approved encryption method (e.g., AES, 3DES, SSH, or SSL).

NET1670: Establish and maintain a standard operating procedure managing SNMP community strings and usernames to include the following:

- Community string and username expiration period
- SNMP community string and username distribution including determination of membership

NET1675: Ensure if both privileged and non-privileged modes are used on all devices. Different community names will be used for read-only access and read-write access.

NET1710: Ensure security alarms are set up within the managed network's framework. At a minimum, these will include the following:

- Integrity Violation: Indicates that network contents or objects are illegally modified, deleted, or added.
- Operational Violation: Indicates that a desired object or service can not be used.
- Physical Violation: Indicates that a physical part of the network (such as a cable) is damaged or modified without authorization.
- Security Mechanism Violation: Indicates that the network's security system is compromised or breached.
- Time Domain Violation: Indicates that an event is happening outside its allowed or typical time slot.

NET1720: Ensure alarms are categorized by severity using the following guidelines:

- Critical and major alarms are given when a condition that affects service has arisen. For a critical alarm, steps must be taken immediately in order to restore the service that is lost completely.
- A major alarm indicates that steps must be taken as soon as possible because the affected service has degraded drastically and is in danger of being lost completely.
- A minor alarm indicates a problem that does not yet affect service, but may do so if the problem is not corrected.
- A warning alarm is used to signal a potential problem that may affect service.
- An indeterminate alarm is one that requires human intervention to decide its severity.

NET1730: Ensure the management workstation is located in a secure environment.

NET1740: Ensure only those accounts necessary for the operation of the system and for access logging are maintained.

NET1750: Ensure a record is maintained of all logons and transactions processed by the management station.

NOTE: Include time logged in and out, devices that were accessed and modified, and other activities performed.

NET1760: Ensure access to the Network Management System (NMS) is restricted to authorized users with individual user IDs and passwords.

NET1762: Ensure all in-band sessions to the NMS are secured using a State-approved encryption method (e.g., AES, 3DES, SSH, or SSL).

NET1770: Ensure connections to the NMS are restricted by IP address to only the authorized devices being monitored.

NET1780: Ensure all accounts are assigned the lowest possible level of access/rights necessary to perform their jobs.

4.9.4 Logistics for Configuration Loading and Maintenance

NET1030: When saving and loading configurations, ensure that the running and startup configurations are synchronized.

NET1040: Ensure at least the current and previous router configurations are stored in a secured location to ensure a proper recovery path.

NET1050: On the system where the configuration files are stored, use the local operating system's security mechanisms for restricting access to the files (i.e., password restricted file access).

NET1060: Do not store unencrypted router passwords in an offline configuration file.

NET1070: Authorize and maintain justification for all Trivial FTP (TFTP) implementations.

NET1071: If TFTP implementation is used, ensure the TFTP server resides on a controlled managed LAN subnet, and access is restricted to authorized devices within the local enclave.

NET1080: Ensure the FTP username and password are configured.

4.9.5 Change Management and Configuration Management

Change management is the formal review process that ensures that all changes made to a system receive formal review and approval. Change management reduces impacts from proposed changes that could possibly have interruptions to the services provided.

NET1110: Ensure all changes and updates are documented in a manner suitable for review and audit.

NET1111: Ensure request forms are used to aid in recording the audit trail.

NET1113: Ensure current paper or electronic copies of configurations are maintained in a secure location.

NET1114: Ensure only authorized personnel, with proper verifiable credentials, are allowed to request changes to routing tables or service parameters.

4.10 AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING (AAA)

4.10.1 AAA Implementation

NET0430: Ensure an authentication server is used to gain administrative access to all network devices.

NET0431: Ensure all AAA authentication services are configured to use two-factor authentication during normal operation.

NET0432: Ensure the device is configured to use AAA tiered authorization groups for management authentication.

NET0433: Ensure an authentication method list is applied to all interfaces via an explicit definition or by use of default key word.

NET0434: Ensure the AAA authentication method implements user authentication.

4.10.2 Administrator Accounts

NET0460: Ensure each user accessing the device locally have their own account with username and password.

NET0465: Ensure all user accounts are assigned the lowest privilege level that allows them to perform their duties.

NET0470: Immediately remove accounts from the authentication server or device when no longer required.

4.10.3 Emergency Account

NET0440: Ensure only one account is defined locally for use in an emergency (i.e., authentication server or connection to the device is down).

NET0441: Ensure the emergency account defaults to the lowest authorization level and the password is in a locked safe.

NET0340: Deploy warning banners on all network devices allowing SSH, Telnet, FTP, or HTTP access.

4.10.4 Two-Factor Authentication

NET0445: To ensure the proper authorized network administrator is the only one who can access the device, ensure device management is restricted by two-factor authentication (e.g., PKI or alternate token logon).

4.10.5 Auditing

Logging is a key component of any security architecture and is a critical part of router security. It is essential security personnel know what is being done, attempted to be done, and by whom in order to compile an accurate risk assessment.

NET1020: Ensure all attempts to any port, protocol, or service that is denied is logged.

NET1021: Configure all devices to log severity levels 0 through 7 and send log data to a syslog server.

NET1022: Ensure the syslog server is only connected to the management network.

NET1023: Ensure the syslog servers are configured in accordance with the appropriate operating system standards/baseline.

NET1025: Ensure a centralized syslog server is deployed and configured by the syslog administrator to store all syslog messages for a minimum of 30 days online and then stored offline for one year.

NET1027: Configure the syslog sever to collect syslog messages from levels 0 through 7.

NET1028: Configure the syslog server to accept messages only from authorized devices (restricting access via source and destination IP address).

NET1280: Ensure there is a review on a daily basis, of the log data by the SA or other qualified personnel, to determine if attacks or inappropriate activity has occurred.

NET1281: Ensure a host intrusion detection system (HIDS) is implemented on the syslog server to provide access control for the syslog data as well as provide the necessary protection against unauthorized user and service access.

NET1284: Ensure configuration data is backed up weekly and whenever configuration changes occur.

NET1286: Ensure the audit log data is backed up weekly.

NET1287: Ensure audit logs are protected from deletion.

NET1288: Ensure the audit trail events are stamped with accurate date and time.

NET1289: Ensure the audit trail events include source IP, destination IP, protocol used and action taken.

NET1300: Ensure administrator logons, changes to the administrator group, and account lockouts are logged.

4.11 PASSWORDS

NET0230: Ensure all communications devices are password protected.

NET0240: Ensure all default manufacturer passwords are changed.

NET0260: Ensure all passwords are created and maintained in accordance with State password standards.

NET0270: Record the locally configured passwords used on communications devices and store them in a secured manner.

NET0580: Ensure a password is required to gain access to the router's diagnostics port.

NET0590: Ensure the CISCO enable secret password does not match any other username password, enable password, or any other enable secret password.

NET0600: Ensure passwords are not viewable when displaying the router configuration. Type 5 encryption must be used for the enable mode password (i.e., enable secret password).

5. DEFINITIONS:

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 660-02: System Security

6.2 RELATED DOCUMENTS

These National Security Agency (NSA) guides provide security rationale with pertinent references identifying the most useful vendor documentation as well as pointers to related books, vendor documents, standards, and available software.

This guide gives an in-depth view on securing Cisco-based routers:

http://www.nsa.gov/snac/routers/C4-040R-02.pdf

Microsoft Windows 2000 Router Configuration Guide:

http://www.nsa.gov/snac/os/win2k/w2k_router.pdf

Signed by Art Bess, Assistant Director

7. DOCUMENT HISTORY

Version	Release Date	Comments
Original	1/30/2008	